Universidade Federal do Rio de Janeiro

Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais

Humberto Buffoni

UMA PROPOSTA DE GERÊNCIA PARA REDES DE COMPUTADORES

Rio de Janeiro

2013

Humberto Buffoni

UMA PROPOSTA DE GERÊNCIA PARA REDES DE COMPUTADORES

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Orientador:

Moacyr Henrique Cruz de Azevedo, M.Sc., UFRJ, Brasil

Rio de Janeiro

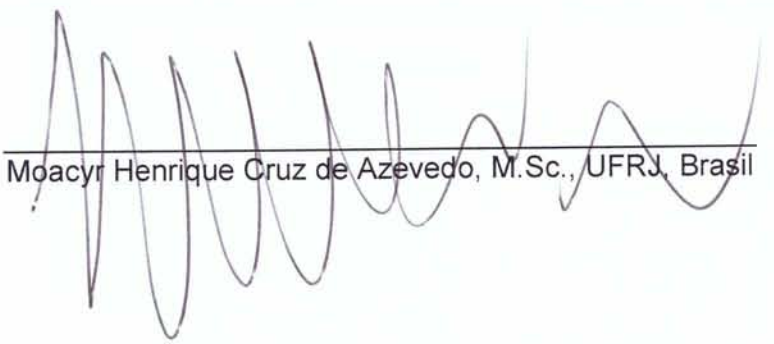
2013

Humberto Buffoni

UMA PROPOSTA DE GERÊNCIA PARA REDES DE COMPUTADORES

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Aprovada em março de 2013.



Moacyr Henrique Cruz de Azevedo, M.Sc., UFRJ, Brasil

Dedico esta monografia a todos os administradores de rede e pessoal de apoio que se esforçam todos os dias para resolver os problemas de todos e muitas vezes não são lembrados.

AGRADECIMENTOS

Agradeço a todos os professores que me acompanharam durante a elaboração desta monografia, em especial ao Prof. Moacyr Henrique Cruz de Azevedo pela paciência e rigor na orientação desta monografia.

RESUMO

BUFFONI, Humberto. **UMA PROPOSTA DE GERÊNCIA PARA REDES DE COMPUTADORES**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2013.

Análise do ambiente de rede com ativos antigos. O objetivo é mapear os problemas relacionados a quedas constantes de acesso à Internet e ao seu desempenho em empresa dentro de uma universidade. Foram utilizadas ferramentas de gerência de rede tais como CACTI, MRTG e PRTG que foram implementadas para análise gráfica de comportamento de rede e seus dispositivos. Também foram empregadas as ferramentas Wireshark e Microsoft Network Monitor para analisar o tráfego de pacotes na rede com o objetivo de identificar falhas e oferecer a melhor solução para a resolução do problema. Todas as ferramentas utilizadas são gratuitas, lembrando o fato, dos limitados recursos para investimento em equipamentos e softwares.

ABSTRACT

BUFFONI, Humberto. **UMA PROPOSTA DE GERÊNCIA PARA REDES DE COMPUTADORES**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2013.

Analysis of the network environment with active network components. The goal is to map the problems related to falls constant Internet access and your performance in small business in the a university. We used network management tools such as CACTI, MRTG and PRTG that were implemented for graphical analysis of network behavior and its devices. We also employed the tools Wireshark and Microsoft Network Monitor to analyze packet traffic on the network in order to identify gaps and provide the best solution to solve the problem. All tools used are free, remembering the fact of limited resources for investment in equipment and software.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

CLI	Command Line Interface
FCAPS	Fault, Configuration, Accounting, Performance and Security
GNU	General Public License
GUI	Graphical User Interface
IETF	Internet Engineering Task Force
IP	Internet Protocol
MIB	Management Information Base
MRTG	Multi Router Traffic Grapher
MTU	Maximum Transmission Unit
NMS	Network Management Stations
PRTG	Paessler Router Traffic Grapher
QoS	Quality of Service
SMI	Structure of Management Information
SNMP	Simple Network Management Protocol
TCP-IP	Transmission Control Protocol – Internet Protocol
TI	Tecnologia da Informação
VoIP	Voice over Internet Protocol
WMI	Windows Management Instrumentations

SUMÁRIO

1 **INTRODUÇÃO**

As redes atuais de computadores são compostas por uma grande variedade de dispositivos que tem como objetivo a comunicação e o compartilhamento de recursos. Na maior parte dos casos, a eficiência dos serviços prestados está associada ao bom desempenho dos sistemas da rede. A grande maioria das organizações dependem destes equipamentos de rede e de um conjunto complexo de servidores para garantir que os dados do negócio possam fluir sem problemas entre os funcionários, escritórios e seus clientes. O sucesso econômico de uma empresa depende, e está fortemente ligada, ao fluxo de informação. Confiabilidade da rede de computadores, velocidade e eficiência são itens cruciais para as empresas realizem bem seus negócios, pois estão altamente dependentes dos ambientes de TI.

Porém, falhas podem ocorrer, seja uma falha física ou por mau funcionamento de softwares, causando prejuízos financeiros. Segundo um estudo realizado pela Universidade de Austin, EUA, o impacto de uma falha de rede produz um decréscimo na receita e aumenta o custo de uma empresa. Conforme esse estudo, o custo de uma falha na rede varia de 2% da receita anual, no primeiro dia da paralisação até cerca de 30%, no trigésimo dia [CARVALHO, 1993].

Considerando este quadro, torna-se cada vez mais necessário o gerenciamento do ambiente de redes de computadores para mantê-lo funcionando corretamente. Surge então a necessidade de buscar uma maneira consistente de realizar o gerenciamento de redes para, com isso, manter toda a estrutura funcionando de forma a atender as necessidades dos usuários e às expectativas dos administradores.

O gerenciamento de redes tem por objetivo controlar e monitorar os ativos da rede para garantir um bom funcionamento para seus usuários. Atualmente tem se tornado de fundamental importância para as empresas essa necessidade de interconexão dos módulos processadores, para que haja o compartilhamento de recursos de hardware e software e também as trocas de informações entre os usuários.

Conforme [TANENBAUM,2003], geralmente uma rede com baixo desempenho é motivo de reclamação por seus usuários, considerando as variadas soluções possíveis, uma delas é a mais usada e consiste em utilizar um computador que interage com os diversos componentes da rede para deles extrair as informações necessárias ao seu gerenciamento. O gerenciador de rede visa manter o controle de informações estratégicas, controlar a complexidade da rede, obter melhorias nos serviços, reduzir ao máximo o tempo de indisponibilidade de sistemas e diminuir os custos com a manutenção de rede. Todos esses esforços são voltados para maximizar a sua eficiência e produtividade. Porém, para que tudo isso ocorra, é necessário o uso de ferramentas de gerência e monitoramento de rede para auxiliar o responsável por essa tarefa de gerenciamento de uma rede. Existem inúmeros tipos de ferramentas no mercado, desde as gratuitas até as que são comercializadas, ferramentas mais simples de trabalhar que somente identificam as ocorrências críticas e realizam o *polling* na rede, como também ferramentas de gerenciamento que auxiliam na detecção de falhas, análise e monitoramento de rede.

> “Gerenciamento de Redes inclui o fornecimento, integração e coordenação de hardware, software e elementos humanos para monitorar, testar, configurar, consultar, analisar, avaliar e controlar a rede e recursos para atender os requisitos de desempenho, qualidade de serviço e

> operação em tempo real dentro de um custo razoável” [KUROSE, 2005].

O Capítulo 2 descreve o referencial teórico desta monografia. A seguir, o Capítulo 3 apresenta o desenvolvimento, análise e a implementação das ferramentas de gerência, e no Capítulo 4 descreve-se os resultados obtidos. Por fim, é apresentada a conclusão.

2 **REFERENCIAL TEÓRICO**

As redes de computadores atuais são compostas por inúmeros dispositivos que precisam estar interligados, para que haja o compartilhamento de informações e também de recursos disponíveis, agilizando os processos para as pessoas e organizações. Os ativos de TI tornam-se cada dia mais essenciais para realização de quaisquer tarefas, por esse motivo, a importância da utilização de ferramentas de gerência e monitoramento de redes.

2.1 GERÊNCIA DE REDES

Gerência de redes é o monitoramento de qualquer estrutura física e/ou lógica de uma rede. É de extrema importância esse gerenciamento para que se obtenha um bom fluxo no tráfego das informações, que os recursos sejam corretamente utilizados e não sobrecarregados, e que os dados sejam transportados com confiabilidade e segurança. Tem por atividade básica detectar falhas e corrigi-las em tempo hábil prevendo também problemas futuros, sem que haja prejuízo no monitoramento. A equipe de TI é responsável por toda a parte de monitoramento da rede, porém precisa ter um bom conhecimento em todas as especificações de hardware e software dos servidores e estações de trabalho. Esta equipe deverá reconhecer os equipamentos, tais como roteadores, *switches*, repetidores entre outros dispositivos que estarão conectados à rede.

A gerência de redes possui quatro elementos básicos:

- Gerente
- Agente
- MIB
- Protocolo de gerenciamento

Gerente é um único computador conectado à rede que executa o *software* de gerenciamento que solicita informações aos agentes. O sistema de gerenciamento também é chamado de console de gerenciamento.

Agente é um *software* que roda em um recurso, elemento ou sistema gerenciado, que exporta uma base de dados de gerenciamento (MIB) para que o gerente possa ter acesso ao mesmo.

MIB (*Management Information Base*) é o conjunto dos objetos gerenciados que procura abranger todas as informações necessárias para a gerência da rede, possibilitando, assim, a automatização de grande parte das tarefas de gerência.

Protocolo de gerenciamento informa os mecanismos de comunicação entre o gerente e o agente. [CARVALHO, 1993]

2.2 MODELOS DE GERÊNCIA DE REDES

Para que haja êxito no funcionamento e eficiência de um sistema de gerenciamento de redes é necessário utilizar os principais componentes de um sistema de gerência de redes que são: Gerência de Falhas, Gerência de Configuração, Gerência de Contabilização, Gerência de Desempenho, Gerência de Segurança. A figura1 relaciona todos os componentes do modelo FCAPS de gerência de redes.

2.3 MODELO FCAPS

Gerenciar conforme o modelo FCAPS (*Fault, Configuration, Accounting, Performance and Security*) foca em como encontrar formas de resolver as questões que envolvem configuração, falhas, desempenho, segurança e

contabilizações relativas à rede. Para que isso ocorra de uma forma padronizada foram criadas dentro do modelo áreas que são chamadas funcionais. A figura 1, representa essas áreas do modelo FCAPS.

Figura 1 - Referência ao nome do modelo FCAPS

O modelo recebe este nome, porque é criado a partir das iniciais de cada área do gerenciamento:

- Gerência de Falhas: Auxilia a encontrar as falhas descobertas na rede. Tem por função detectar, isolar e solucionar o problema.
- Gerência de Configuração: Auxilia a descobrir a configuração de todos os dispositivos que estão relacionados à rede em questão. Busca informações sobre as configurações, geração de eventos, atribuição de valores iniciais aos parâmetros, registro de informações, alteração de configuração, e início e encerramento de operação dos elementos gerenciados.
- Gerência de Contabilidade: Determina quais serão as formas e acessos que os usuários terão disponíveis. Tem como função a coleta de informações sobre utilização, estabelecimento de cotas de utilização e escala de tarifação, e aplicação de tarifas e faturamento.
- Gerência de Desempenho: Relacionada diretamente com a qualidade de serviço da rede. A gerência de desempenho necessita planejar a

capacidade da rede para manter e prestar suporte para todos os usuários. Utiliza-se de indicadores para monitoramento de rede.

- Gerência de Segurança: É o controle de todos os acessos à rede. Protege os elementos e detecta possíveis tentativas de invasão.[CARVALHO, 1993]

2.4 PROTOCOLO DE GERENCIAMENTO - SNMP

O SNMP (*Simple Network Management Protocol*) foi criado em 1988 para suprir a necessidade de padronizar o processo de gerenciamento de dispositivos, facilitando o gerenciamento remoto desses dispositivos por meio de um conjunto de regras e processos. Com o SNMP é possível gerenciar inúmeros tipos de ativos da rede, como por exemplo roteadores, *switches*, impressoras, *no-breaks*, servidores, entre outros. Pode ser utilizado para sistemas, tais como *Unix*, *Windows*, dentre outros. O SNMP visa à redução dos gastos com a construção de um agente que consiga suportar o protocolo em questão e também aceita a inclusão de novos objetos e características. Outro objetivo é tentar diminuir o tráfego das mensagens de gerenciamento através da rede que gerencia os recursos.

> "O núcleo SNMP é um conjunto simples de operações (e das informações obtidas por essas operações) que permitem ao administrador modificar o estado de alguns dispositivos baseados em SNMP." [MAURO e SCHMIDT, 2001].

O protocolo SNMP possui duas entidades: gerenciadores e agentes. Gerenciador usualmente é um servidor que executa programas com objetivo de gerenciar uma rede. Também conhecido como NMSs (*Network Management Stations*) tem por tarefa receptar as informações emitidas pelos agentes. Um NMS

tem por tarefa as operações de *polling* e recepção dos *traps* de agentes da rede.

Os agentes são os módulos do programa de gestão hospedado no dispositivo. Monitoram a rede, traduzindo e enviando as informações coletadas ao gerenciador. O *poll* é toda a consulta de informações de um agente, que podem ser servidores, roteadores, comutadores, entre outros. Todas as informações que forem coletadas podem ser utilizadas para detecção de alguma operação errônea na rede. A *trap* é utilizada pelo agente para comunicar à NMS que algo ocorreu. As *traps* são emitidas em modos assíncronos, ou seja, não servem para atender às solicitações e consultas da NMS. [MAURO e SCHMIDT, 2001]

2.4.1 **Operações de gerência do SNMP**

As operações do SNMP têm por objetivo a troca de informações entre o gerente e o agente sobre os objetos gerenciados no ativo monitorado. Uma das principais características do protocolo SNMP é ser simples, pois possui um pequeno conjunto básico de operações baseado no paradigma conhecido como “busca-armazenamento”, isso quer dizer que as operações do protocolo SNMP são derivadas de operações básicas de busca e armazenamento. [CARVALHO, 1993]

A figura 2, a seguir, apresenta as operações básicas do protocolo SNMP, a interação e uma pequena descrição de cada operação.

Operação	Interação	Descrição
GetRequest GetNextRequest GetBulkRequest	Gerente-agente	Solicitação de leitura sobre o conteúdo dos objetos: • Apenas uma instância de objeto • Próximo na lista • Bloco
InformRequest	Gerente-agente	Indica o valor da MIB disponível a partir da versão dois do SNMP.
SetRequest	Gerente-agente	Define valor da MIB.
Response	Agente-gerente	Retorna o conteúdo do valor em resposta ao pedido do gerente.
Trap	Agente-gerente	Informa o gerente a ocorrência de um evento excepcional, como por exemplo, LINK DOWN.

Figura 2 - Operações do SNMP

2.4.2 **Versões do SNMP**

SNMP versão 1 (SNMPv1) possui três documentos: RFC 1155 define os mecanismos usados para descrever e nomear os objetos que serão gerenciados; RCF 1157 define SNMP (*Simple Network Management Protocol*); e RCF 1212 define um mecanismo de descrição mais conciso, porém é inteiramente consistente ao SMI (*Structure of Management Information*). A segurança do SNMPv1 baseia-se em comunidades, que são nada mais do que senhas que permitem que qualquer aplicativo baseado em SNMP tenha acesso a informações de gerenciamento de um dispositivo. Geralmente existe três comunidades no SNMPv1 read-only, read-write e *trap* [MAURO e SCHMIDT, 2001].

SNMP versão 2 (SNMPv2) é definida nas RFCs 1902, 1903, 1904, 1905, 1906 e 1907. É frequentemente citada como SNMPv2 baseado em *strings* de comunidade. O SNMPv2 acarreta em algumas vantagens, como melhorias na eficiência e no desempenho, como o operador *get-bulk*, notificação de evento confirmado, como o operador *inform,* e maior detalhamento de erros.

SNMP versão 3 (SNMPv3) é definida nas RFCs 1905, 1906, 1907, 2570, 2571, 2572, 2573, 2574, 2575, 2576 e 2786. Nas versões anteriores não havia uma preocupação especifica com segurança. No SNMPv3 não há alterações no protocolo, porém há a inclusão de uma autenticação rigorosa e comunicação privativa entre as entidades gerenciadas. Apenas a atribuição de senhas não provê garantias de segurança na rede [MAURO e SCHMIDT, 2001].

> Segundo [Mauro e Schmidt, 2001], "*Simple Network Management Protocol* SNMPv3 lida com os problemas de segurança que infestaram SNMPv1 e SNMPv2. Para todos os objetivos práticos a segurança é a única questão que o SNMPv3 endereça. Não ocorreram novas alterações no protocolo nem existem operações novas. O SNMPv3 tem suporte para todas as operações definidas nas versões 1 e 2."

2.4.3 **Banco de dados - MIB (Management Information Base)**

O MIB (*Management Information Base*) é o banco de dados de todos os dispositivos gerenciados que o agente monitora. Tem por objetivo definir um nome, em texto, de um dos objetos que estão sendo gerenciados e trazer a explicação de seu significado. Existem dois tipos de versão da MIB: a MIB-1 que é da versão 1 e a MIB-2 que é da versão 2. A MIB-1 é a original, porém, após a implementação da MIB-2, esta não é mais consultada, sendo somente a MIB-2 utilizada atualmente. Os agentes podem instalar inúmeras MIBs, porém é necessário que seja implantada uma MIB especifica MIB-2. Nesta MIB são

encontrados todos os dados estatísticos necessários, tais como unidade fundamental de transferência de rede TCP/IP, octeto, velocidade da interface, MTU, entre outras. A MIB-2 visa apresentar todas as informações sobre o gerenciamento de TCP/IP.

Para [Harnedy, 1997], as MIBs, ou bases de informações de gerência, são compostas pelas informações de gerenciamento e pelos objetos gerenciados. Um objeto gerenciado é definido como a unidade da informação de gerenciamento.

2.5 FERRAMENTAS DE GERÊNCIA DE REDES

Para monitorar e controlar os elementos da rede, os administradores de redes são geralmente auxiliados por um sistema de gerência que pode ser definido como uma coleção de ferramentas integradas para monitoração e controle da rede. Este sistema oferece uma interface única, com informações sobre a rede, podendo oferecer um conjunto poderoso e amigável de comandos que são usados para executar quase todas as tarefas da gerencia da rede. [STALLINGS, 1996]

Existe grande variedade de ferramentas de gerência de redes disponíveis que auxiliam no gerenciamento de uma rede, algumas chamadas de ferramentas de monitoramento gráfico, utilizadas para apresentar através de gráficos os dados coletados para monitoração e análise de comportamento de rede; e outras chamadas de *Sniffers*, utilizadas para verificar e analisar os protocolos e os pacotes enviados e recebidos pelos ativos na rede. Nas duas seções a seguir serão apresentadas as ferramentas de análise gráfica MRTG, CACTI, PRTG, e as ferramentas de análise de pacotes (*Sniffers*) *Wireshark* e *Microsoft Network Monitor*.

2.5.1 **Ferramentas de Análise Gráfica do Comportamento de Rede e Seus Dispositivos**

MRTG foi desenvolvido por Tobias Oetiker e atualmente se encontra na versão 2.17.4. É uma ferramenta de monitoramento de rede escrito em Perl e liberado sob a licença GNU (*General Public License*) que tem como principal objetivo monitorar a carga de tráfego em enlaces de rede. Também é possível configurá-la para coletar dados sobre utilização de memória, utilização de disco e média de carregamento. MRTG gera gráfico diário, semanal, mensal e anual demonstrando os dados coletados que podem ser visualizados de qualquer navegador e funciona na maioria das plataformas *Unix* e *Windows*. O MRTG não detecta nem soluciona problemas na rede, não possui a capacidade de gerar alarmes ou processar *traps*, nem a opção de definir objetos. É apenas usado para oferecer uma visão gráfica do desempenho da rede e para a compreensão e análise do comportamento dos elementos monitorados na rede. [MRTG, 2012]

CACTI foi desenvolvido inicialmente por Ian Berry e atualmente se encontra na versão 0.8.8a. É uma interface completa (*Front-End*) escrito na linguagem PHP para *RRDTool*, responsável por armazenar os dados coletados e por gerar os gráficos num banco de dados MySQL. A ferramenta CACTI funciona nas plataformas *Linux* e *Windows* e foi liberada sob a licença GNU (*General Public License*), e usada para monitorar os ativos da rede fornecendo em forma de gráficos os dados recolhidos como tráfego de rede, espaço em disco, uso de memória física e memória virtual, uso de CPU, entre outros. [CACTI, 2012]

PRTG *Network Monitor* é uma ferramenta de monitoramento de rede, é o sucessor do PRTG *Traffic Grapher*, atualmente se encontra na versão

12.2.1.1767. Os desenvolvedores da ferramenta recomendam que para o bom funcionamento é necessário ser instalada em uma estação com sistema operacional Microsoft Windows. O PRTG *Network Monitor* é utilizado para monitoramento de redes das pequenas, médias e grandes empresas; pode monitorar sistemas Linux, clientes Windows, roteadores, *switches*, servidores de arquivos, e-mails, disponibilidade da rede, uso de banda, qualidade de serviço, carga de memória, uso de CPU, entre outros. O PRTG suporta protocolos SNMP (*Simple Network Management Protocol*), WMI (*Windows Management instrumentations*), *packet sniffer*, NetFlow, sFlow, jFlow. A coleta de dados sobre a disponibilidade da rede e os parâmetros é feita 24 horas por dia e é armazenado em um banco de dados interno, que pode ser consultado depois para análise. Os desenvolvedores no site da própria ferramenta (www.paessler.com.br/PRTG), disponibilizam quatro tipos diferentes de licenças que são:

- *Freeware Edition*: Para uso pessoal ou comercial até 10 sensores, suporta todos os sensores disponíveis, com intervalo de monitoramento mínimo de 1 minuto;
- *Starter Edition*: Possui todas as características da edição Freeware, mas a diferença de que os sensores podem ser estendidos até 20;
- *Trial Edition*: É uma edição para fins de avaliação, destinada a aqueles clientes que estão interessados em aquisição de licenças comerciais. Possui número ilimitado de sensores e suporta todos os sensores disponíveis, com intervalo de monitoramento mínimo de 1 segundo. O período de avaliação é de 30 dias. Vale ressaltar que essa edição necessita de uma chave de licença temporária que tem que ser solicitada no site da própria ferramenta;

- *Comercial Edition*: Possui várias licenças para atender às necessidades das pequenas, médias e grandes organizações, suporta todos os tipos de sensores disponíveis, com intervalo de monitoramento mínimo de 1 segundo. O valor das licenças varia de US$ 400,00 até US$ 32.400,00. [PRTG, 2012].

2.5.2 **Analisadores de Pacotes (*Sniffers*)**

Sniffers são ferramentas de análise de rede que têm como objetivo interceptar e registrar o tráfego de dados em uma rede. Os *sniffers* são capazes de capturar, decodificar e apresentar os dados de uma forma clara e de fácil compreensão. Também são capazes de analisar a atividade da rede que envolve protocolos específicos, e gerar e exibir estatísticas. Um *sniffer* geralmente possui um filtro que auxilia os administradores de rede a capturar apenas o tráfego relevante ao problema a ser resolvido, diminuindo os pacotes capturados e apresentando apenas os dados relevantes.

Wireshark é um analisador de pacotes de rede. Identifica, reconstrói, organiza e disponibiliza os dados capturados de forma visual e hierarquizada, através de uma interface de usuário, que pode ser através linha de comando, como o TShark versão CLI - *Command Line Interface* do *Wireshark,* ou através de GUI - *Graphical User Interface*. É uma ferramenta poderosa na análise de rede, possibilita uma forma completa e eficiente de resolver problemas de rede, dos mais básicos até os mais avançados. Possui um avançado mecanismo de filtros, permitindo uma análise mais criteriosa, precisa e eficaz. Disponível para os ambientes *Unix* e *Windows*, foi desenvolvida por Gerald Combs. A primeira versão da ferramenta (0.2.0) inicialmente chamada (*Ethereal*) foi lançada em 1998

sob GNU GPL (*General Public License*). Em 2008, e após dez anos de desenvolvimento, foi lançada a versão completa 1.0, e atualmente se encontra na versão 1.8.3. [WIRESHARK, 2012]

Microsoft Network Monitor está disponível desde as primeiras versões de *Windows*, como o *Windows for Workgroups* 3.11, e atualmente se encontra na versão 3.4. É uma ferramenta de diagnóstico que captura pacotes de rede examinando-os, traçando-os e gerando estatísticas, permitindo análise desses pacotes para detectar a causa de determinadas falhas ou lentidão no tráfego que pode vir a causar interrupção de serviços importantes e essenciais da rede. O *Network Monitor* é uma peça primária para se criar linhas de base dos fluxos de informações da rede. [MICROSOFT, 2012]

3 **DESENVOLVIMENTO**

Esta monografia apresenta um estudo de caso realizado em uma empresa com filial situada em Rio de Janeiro/RJ com atuação no ramo prestação de serviços. A empresa não possui ferramentas de monitoramento de rede ou análise de tráfego. Após fazer um levantamento com base num questionário respondido pelos funcionários, foi constatado que em determinados períodos do dia os usuários enfrentam problemas no desempenho da rede, tais como lentidão e quedas constantes de conexão internet. Portanto, é necessário monitorar os ativos da rede e analisar o tráfego para identificar o que realmente está ocasionando tal problema neste ambiente. Para após a análise do ambiente e identificação da causa, aplicar a melhor solução a fim de neutralizar definitivamente o problema.

Serão utilizadas as ferramentas MRTG, CACTI e PRTG para monitoramento da estrutura da rede e a coleta de dados para identificação de fluxo de dados, para depois de verificado no ambiente, apresentar qual dessas ferramentas melhor atendeu às necessidades para identificação do comportamento da rede nesta organização. Para análise do tráfego serão implantadas as ferramentas de *sniffer Wireshark* e *Microsoft Network Monitor* a fim de identificar a real causa do comportamento não usual da rede, desta forma, sendo possível mapear a origem do problema e neutralizá-lo.

3.1 ANÁLISE DO AMBIENTE

Conforme ilustrado na figura 3, o cenário problemático consiste em um servidor, com sistema operacional *Microsoft Windows Server* 2003 - Saturno, um servidor *Unix Freebsd* – Júpiter, e doze estações de trabalho distribuídas com nome de luas: Titan, Phobos, Deimos, Uranus, Ganymede, Encelado, Febe, Rea,

Telesto, Hiperion, Tetis e Pan sendo que, nove computadores *desktops* e dois *notebooks* utilizam o sistema operacional *Microsoft Windows* XP Professional SP3 e um notebook utiliza o sistema operacional *Microsoft Windows* Seven Professional. O parque computacional da empresa em questão também possui um *hub switch* de 16 portas *Encore* 10/100 Mbps não gerenciável, como também possui um enlace para acesso à internet fornecido pela universidade de 100 Mbps T1 LAN.

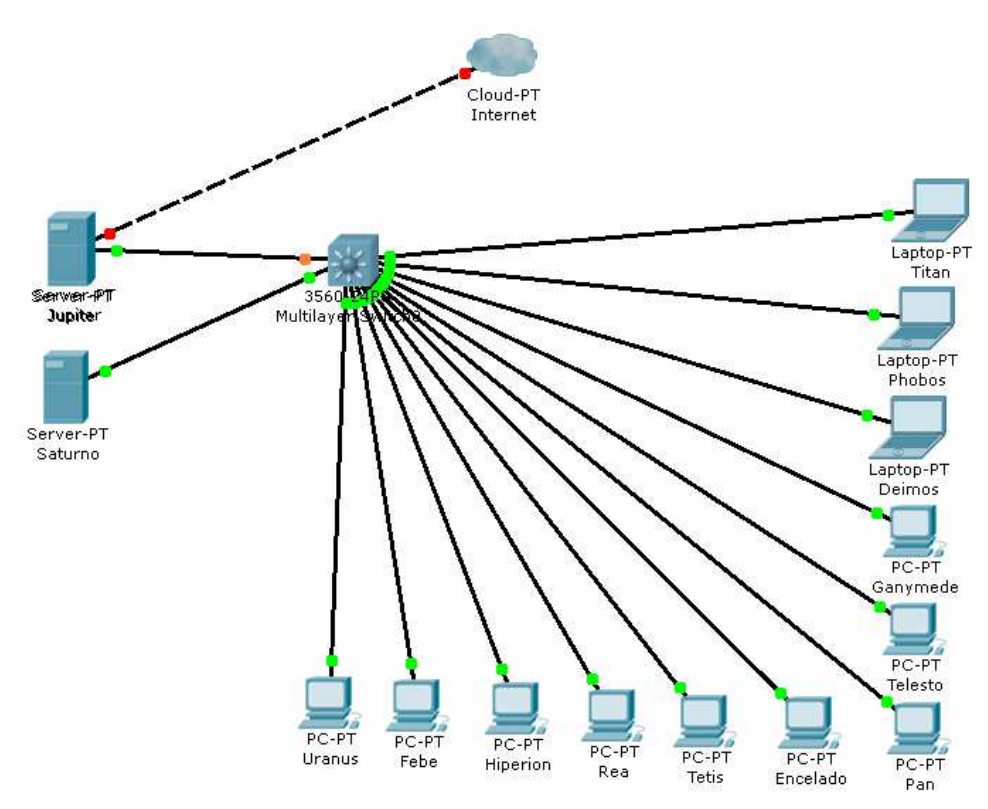


Figura 3 - Topologia lógica da rede

3.2 IMPLEMENTAÇÃO

No ambiente desta empresa foram instaladas as ferramentas MRTG, CACTI e PRTG *Network Monitor* que monitoram o tráfego da rede usando o protocolo de gerenciamento SNMP, protocolo de gerência de rede padrão do IETF (*Internet*

Engineering Task Force). O SNMP por padrão utiliza as portas UDP 161 para agente e UDP 162 para gerente, portanto houve a necessidade de, antes da instalação, liberar a porta UDP 161 nos firewalls de cada estação e UDP 162 no servidor (Saturno). Também foram implementados dois *sniffers*, *Wireshark* e *Microsoft Network Monitor*, que analisarão o tráfego e auxiliarão na descoberta do que realmente está consumindo a banda e ocasionando a lentidão de acesso à *internet*. O próprio servidor da empresa foi utilizado para a instalação das ferramentas citadas. Este servidor possui o sistema operacional *Microsoft Windows Server Enterprise Edition* SP2, Processador Dual Xeon 3.6GHz e 6 GB de Memória RAM.

3.3 INSTALAÇÃO DA FERRAMENTA MRTG

Para instalação desta ferramenta foi utilizada a última versão liberada dia 12.01.2012, que pode ser encontrada no site da própria ferramenta acessando http://oss.oetiker.ch/mrtg/pub/?M=D e efetuando o *download* do arquivo mrtg-2.17.4.zip. Por ser desenvolvida em Perl foi necessário a utilização do pacote ActivePerl-5.16.1.1601-MSWin32-x86-296175.msi para utilização do MRTG, que pode ser encontrado em: http://www.activestate.com/activeperl/downloads. A instalação da ferramenta MRTG ocorreu de maneira simples e relativamente fácil, pois, para instalar o pacote Perl, é necessário acessar o diretório em que foi feito o *download* e executar o arquivo *installer*. No momento da instalação da MRTG é preciso descompactar o *mrtg-2.17.4.zip* e será criada no diretório principal a pasta mrtg-2.17.4, através do prompt de comando, ingressar na pasta c:\mrtg-2.17.4\bin e executar Perl MRTG. Com o MRTG instalado, o próximo passo é adicionar os ativos da rede em que o tráfego de entrada e saída de cada interface desses ativos

será monitorado. Para que isso ocorra é necessário saber o endereço IP ou nome do *host* e a comunidade de leitura de cada dispositivo. A figura 4 ilustra os dispositivos da rede que foram adicionados. Estes são todos os *hosts* que fazem parte da rede local desta organização.

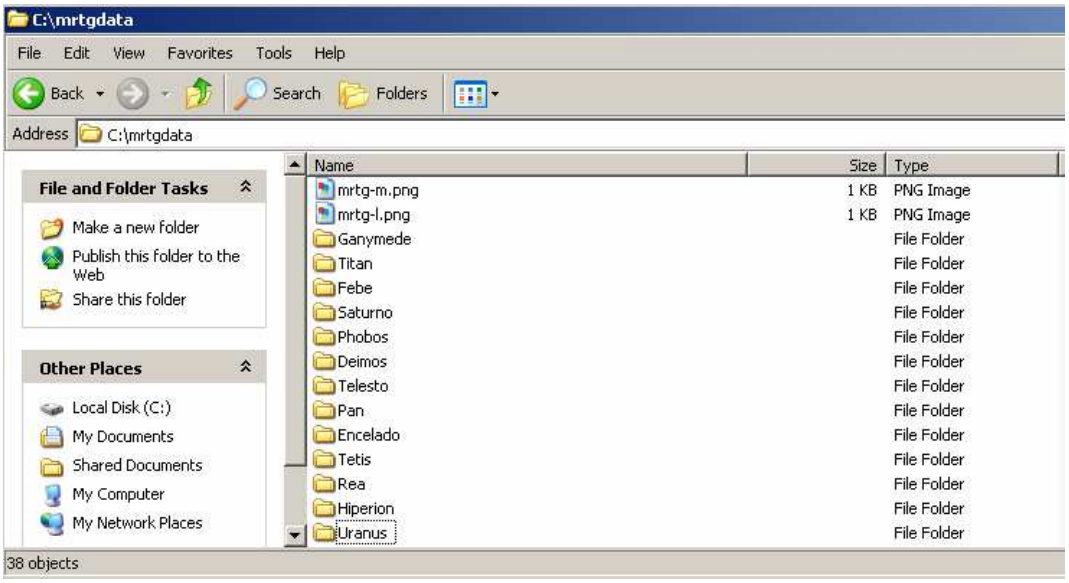


Figura 4 - Dispositivos da rede monitorados pela ferramenta MRTG

3.4 INSTALAÇÃO DA FERRAMENTA CACTI

Para a instalação da ferramenta CACTI foi utilizada a versão 0.8.8a que se encontra disponível para o *download* acessando http://www.cacti.net/downloads e obtendo o arquivo cacti-0.8.8a.zip. O CACTI requer que os seguintes *softwares* estejam instalados no servidor: RRDTools, MySQL, PHP, *net-snmp* e um servidor *web* que suporte PHP, como Apache ou IIS. Não serão abordados detalhes da instalação da ferramenta CACTI pois o site da própria ferramenta possui uma vasta documentação para este fim e disponibiliza um passo a passo sobre como deve ser feita a instalação. Para maiores esclarecimentos é necessário acessar o endereço: http://www.cacti.net/downloads/docs/html/install_windows.html. Cabe ressaltar que

está disponível também a mesma versão do CACTI com os *softwares* RRDTools, MySQL, PHP, net-snmp e servidor *web*, e pode ser encontrada no site http://www.cacti.net/downloads/packages/Windows/. Basta efetuar o *download* do arquivo `Cacti-0.8.8a.exe` e executá-lo que a ferramenta será instalada juntamente com os *softwares* requeridos. Com o CACTI e seus softwares instalados, é necessário cadastrar os dispositivos da rede que serão monitorados. O cadastramento é efetuado de forma simples, conforme ilustrado na figura 5. Basta acessar a interface web da própria ferramenta e clicar em *console* e depois *devices*, após clicar em *new*, será aberta uma janela solicitando algumas informações necessárias sobre o novo dispositivo, tais como descrição do dispositivo, nome ou IP, *template* a ser usado, versão do protocolo SNMP, comunidade de leitura e a porta SNMP. São estas as informações básicas que devem ser informadas no momento da criação de um novo dispositivo, ilustrado na figura 5.

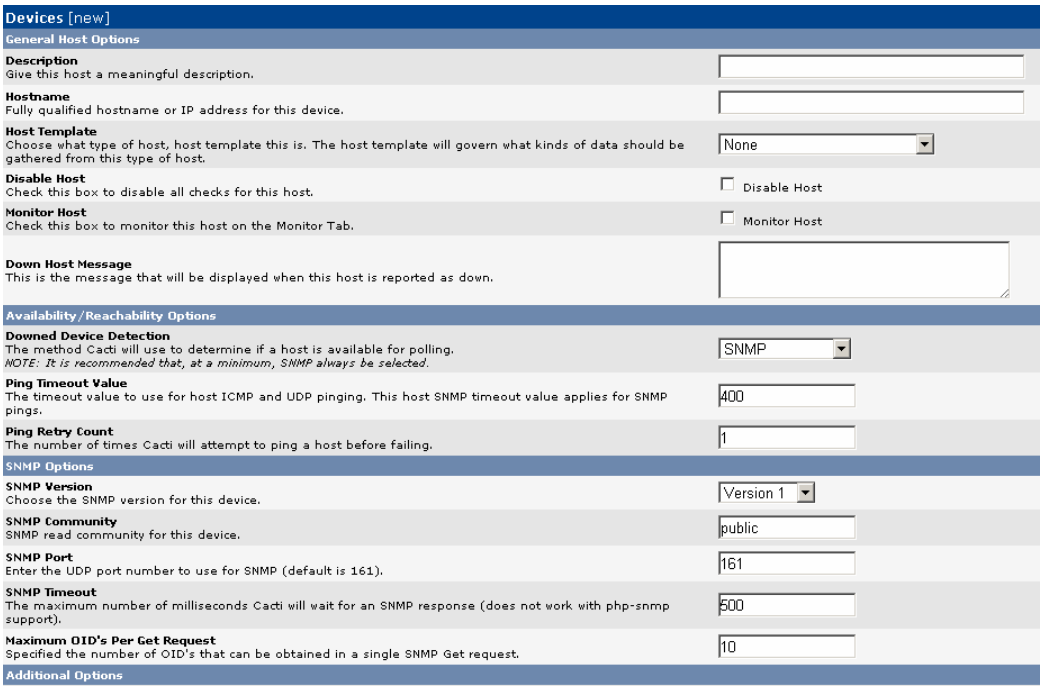


Figura 5 - Tela de cadastro dos ativos na ferramenta CACTI

O CACTI por padrão acompanha uma lista de dispositivos: roteador Cisco, servidor *Linux*, servidor *NetWare* e *Windows* 2000 /XP, e também possui a opção de criar um dispositivo genérico e definir os parâmetros a serem monitorados caso o mesmo não se encontrar na lista. A figura 6 ilustra os dispositivos da rede que foram adicionados.

Figura 6 - Dispositivos da rede monitorados pelo CACTI

3.5 INSTALAÇÃO DA FERRAMENTA PRTG

O site da ferramenta oferece uma versão gratuita de até 10 sensores a serem monitorados, podendo ser estendidas para até 20 sensores. Para isso é necessário colocar o link da própria ferramenta, http://www.paessler.com no site da empresa em que os dispositivos serão monitorados com o logotipo da ferramenta PRTG, e depois enviar um e-mail com o URL da página para sales@paessler.com. Após esse processo é oferecida uma chave de liberação para usar até 20 sensores. O desenvolvedor da ferramenta PRTG *Network*

Monitor disponibiliza também no *site* uma versão paga e outra para teste por 30 dias com todas as funcionalidades. A versão utilizada na instalação da ferramenta é 12.2.1.1767 e pode ser encontrada acessando o endereço: http://www.paessler.com/prtg/download. Após obter o arquivo, basta executar a instalação. Para ter acesso à interface *web* da ferramenta, clicar no ícone PRTG *Network Monitor*, criada na área de trabalho. O próximo passo é cadastrar os dispositivos que serão monitorados. Para isso é preciso informar o nome e o IP do dispositivo na rede, um ícone para identificar o dispositivo, e o sensor que será monitorado. A figura 7 ilustra a tela de cadastro dos dispositivos da rede.

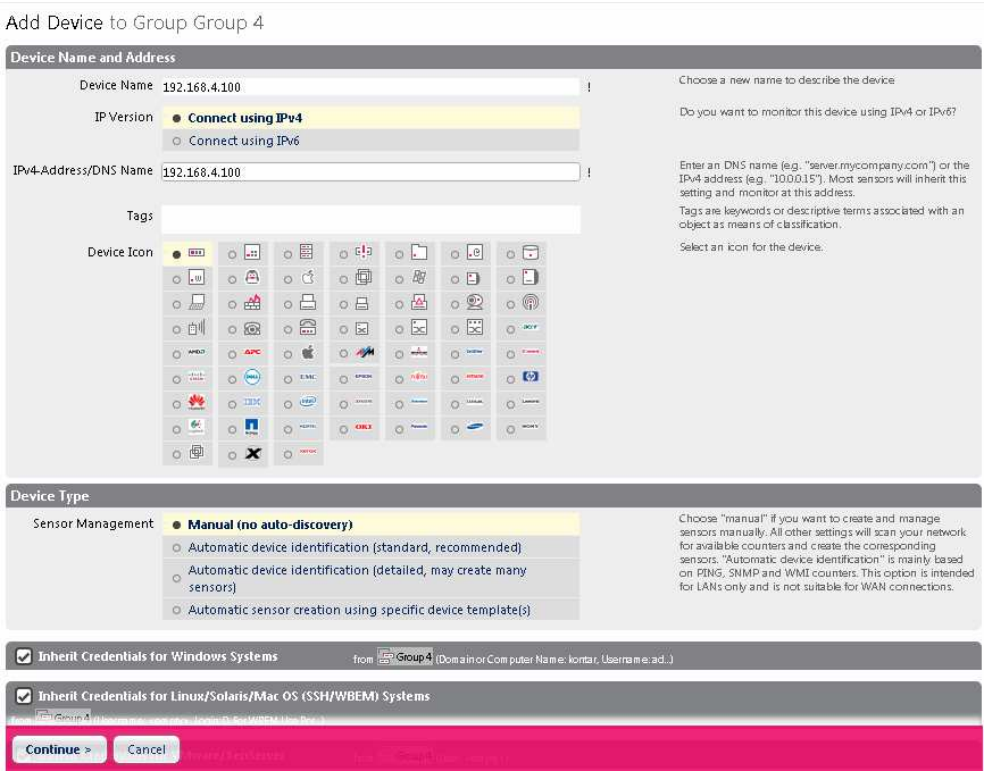


Figura 7 - Tela de cadastro dos ativos na ferramenta PRTG

Após cadastrar os dispositivos, o próximo passo é adicionar os sensores que possibilitam monitorar vários aspectos sobre os dispositivos que necessitam ser

monitorados. A nova versão do PRTG *Network Monitor* disponibiliza mais que 118 diferentes tipos de sensores que foram classificados em grupos para facilitar a procura. Para adicionar um sensor clique em *Add Sensor*, e depois escolha qual dos sensores serão utilizados. A figura 8 ilustra os ativos da rede que serão monitorados pela ferramenta PRTG Network Monitor.

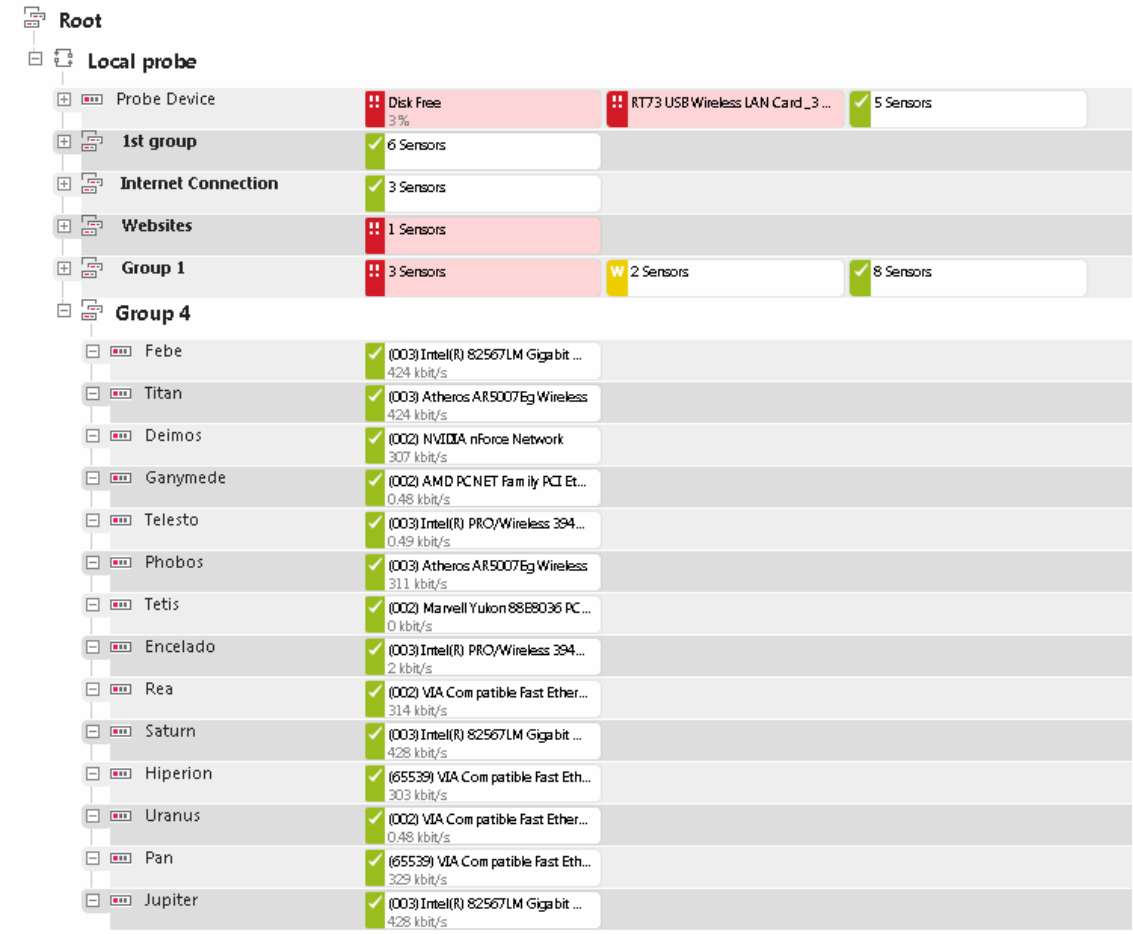


Figura 8 - Dispositivos da rede monitorados pelo PRTG

3.6 INSTALAÇÃO DA FERRAMENTA WIRESHARK

Na instalação da ferramenta foi utilizada a versão 1.8.3 disponibilizada pelo seu desenvolvedor no site da mesma, e pode ser encontrada acessando http://www.wireshark.org/download.html. Para instalar, basta clicar no arquivo

executável baixado (wireshark-win32-1.8.3.exe).

3.7 INSTALAÇÃO DA FERRAMENTA MICROSOFT NETWORK MONITOR

Na instalação da ferramenta *Microsoft Network Monitor* foi utilizada a versão 3.4 que se encontra disponível em: http://www.microsoft.com/download/en/details.aspx?id=4865. Para efetuar a instalação da ferramenta basta executar o arquivo baixado (NM34_X86.exe).

3.8 MONITORAMENTO DOS DADOS

As ferramentas de monitoramento MRTG, CACTI, e PRTG, foram instaladas no servidor Saturno e colocadas para executar ao mesmo tempo para garantir a precisão sobre as informações que se deseja monitorar. Essas ferramentas monitorarão o tráfego de entrada e saída de cada placa de rede das estações de serviço na empresa. As ferramentas foram configuradas para utilizar o protocolo SNMP para realizar a tarefa de coleta de dados, por isso foi necessário antes da coleta ativar o serviço SNMP em cada estação de trabalho, pois, por padrão, esse serviço é incluído no sistema operacional *Windows* desabilitado.

Conforme o levantamento realizado através de questionários com os funcionários da empresa, não há horário específico durante o expediente em que ocorre a lentidão e as quedas constantes de conexão de internet, por isso a decisão de realizar o monitoramento durante todo o horário de funcionamento da empresa sem interrupções de segunda-feira a sexta-feira entre 8h e 19h30min, e aos sábados entre 08h e 15h, no período de uma semana entre os dias 27.10.2012 e 04.11.2012.

3.9 COLETA DOS DADOS

Nesta seção serão apresentados os dados coletados pelas ferramentas de monitoramentos e pelos analisadores de pacotes. Os dados coletados pelas ferramentas MRTG, CACTI e PRTG durante uma semana sobre o tráfego de entrada e saída nas placas de rede dos ativos monitorados foram analisadas e preenchidas em três tabelas, cada qual pertence a uma ferramenta e contém informações do valor máximo de entrada e saída do tráfego coletado por cada ferramenta. Os dados coletados pelas ferramentas de análise de pacotes *Wireshark* e *Microsoft Network Monitor* serão demonstrados posteriormente.

3.9.1 **Dados Coletados pela Ferramenta MRTG**

O MRTG gerou quatro tipos de gráficos para cada ativo monitorado na rede: gráfico diário com média de cinco minutos de coleta, semanal com média de trinta minutos de coleta, mensal com média de duas horas de coleta e anual com média de um dia de coleta. Para preencher a tabela 1 e obter valores mais precisos de tráfego de entrada e saída de cada ativo, foi necessário consultar e verificar todo dia o gráfico diário gerado pela ferramenta MRGT, pois, esse tipo de gráfico é descartado pela ferramenta após vinte e quatro horas de coleta, e não há como fazer consultas precisas.

Tabela 1 – Dados coletados pela ferramenta MRTG

Ativo	Tráfego de entrada Máximo KB/s	Tráfego de saída Máximo KB/s
Deimos	224,4	28,1
Encelado	120,3	12,2
Febe	519,4	31,0
Ganymede	81,7	5,2
Hiperion	34,5	6,7
Jupiter	410,3	56,7
Pan	8,1	1,2
Phobos	16,0	7,2
Rea	32,9	4,5
Saturno	137,2	25,8
Telesto	45,6	34,4
Tetis	54,7	21,3
Titan	56,8	12,4
Uranus	34,9	5,1

3.9.2 **Dados Coletados pela Ferramenta CACTI**

O CACTI possui dois tipos de *pollers* que podem ser utilizados. O primeiro *poller* (cmd.php) é um agente escrito em linguagem PHP, e o segundo *poller* (*spine*) escrito em linguagem C. Para o monitoramento dos ativos, foi definido o uso do *poller* (cmd.php) pois é recomendado para pequenas e medias redes. Para a coleta de dados, o intervalo de *poller* foi definido em 5 minutos. O CACTI utiliza o RRDTool para armazenar os dados necessários na criação dos gráficos, e uma das características do mesmo é que possui um tamanho máximo e não pode ser ultrapassado. Isso quer dizer que os dados numéricos armazenados mais antigos não podem ser recuperados, pois com a passagem do tempo apenas será possível recuperar as médias desses dados numéricos, impedindo a recuperação do valor exato em determinado momento do dia. O CACTI não apresenta os valores coletados em forma de tabelas, então, para ter os valores ilustrados na

tabela 2, foi necessário efetuar uma análise minuciosa de cada um dos gráficos diários com média de 30 minutos de coleta, que foram gerados para cada ativo monitorado na rede da organização.

Tabela 2 – Dados coletados pela ferramenta CACTi

Ativo	**Tráfego de entrada Máximo KB/s**	**Tráfego de saída Máximo KB/s**
Deimos	80,5	4,3
Encelado	50,1	3,4
Febe	502,7	23,2
Ganymede	34,8	23,7
Hiperion	46,7	18,7
Jupiter	140,6	45,4
Pan	7,8	0,8
Phobos	14,7	6,8
Rea	28,9	4,3
Saturno	134,1	24,9
Telesto	35,4	28,7
Tetis	44,5	18,3
Titan	46,9	12,3
Uranus	28,7	4,9

3.9.3 **Dados Coletados pela Ferramenta PRTG**

Para monitorar o tráfego de entrada e saída de cada ativo na rede da empresa através da ferramenta PRTG foi utilizado o sensor *SNMP Traffic*. O PRTG, tal como MRTG e CACTI apresenta o tráfego em forma de gráficos, porém se diferencia e destaca por apresentar também tabelas junto com os gráficos com os dados numéricos sobre o tráfego passante de cada estação. A tabela possui várias colunas com inúmeras informações importantes que auxiliam os administradores da rede a terem idéias mais claras e detalhadas sobre o tráfego. Por exemplo: velocidade e volume total do tráfego, velocidade e volume total de tráfego de entrada, velocidade e volume total de tráfego de saída, entre outros, podendo

consultar essas informações em colunas separadas ou unindo-as na tabela. O PRTG, por apresentar os dados em tabelas, proporciona um alto grau de precisão no momento da consulta dos dados, podendo até recuperar e consultar o tráfego passante em cada ativo por segundos. Os valores apresentados na tabela 3, foram fornecidos pela ferramenta PRTG, definindo o intervalo de coleta de uma hora. A consulta desses valores, analisando a tabela fornecida pelo PRTG, foi rápida, diferentemente da MRTG e CACTI que fornecem os valores coletados apenas através de gráficos, pois exigiram muito mais tempo e atenção para levantar os valores apresentados nas tabelas 1 e 2.

Tabela 3 – Dados coletados pela ferramenta PRTG

Ativo	**Tráfego de entrada Máximo KB/s**	**Tráfego de saída Máximo KB/s**
Deimos	77,1	4,1
Encelado	48,2	3,2
Febe	505,3	28,8
Ganymede	33,9	24,6
Hiperion	43,8	16,5
Jupiter	101,3	44,3
Pan	7,2	0,6
Phobos	15,9	6,3
Rea	26,7	4,5
Saturno	132,9	22,9
Telesto	34,9	23,9
Tetis	42,5	19,1
Titan	43,5	12,1
Uranus	25,6	3,8

3.9.4 **Análise do Resultado das Três Ferramentas**

Com os valores máximos coletados de entrada e saída de tráfego de cada ativo pelas três ferramentas, e preenchidos nas tabelas 1,2 e 3 percebeu-se que a estação de serviço Febe na rede é o ativo em que se alcançou o valor mais alto de tráfego de entrada, comparado com os outros ativos no período de uma semana de monitoramento. Por ser uma estação de serviço localizada na área de pesquisa da empresa, que tem por função preparar e processar todos os dados de entradas e saídas dos projetos, ter um tráfego de entrada muito elevado não é normal, assumindo e a grande parte dos dados é fornecida via CD ou DVD devido as cláusulas de confidencialidade.

Portanto, com a estação Febe identificada como a estação em que houve maior consumo de banda em toda a empresa durante o período de monitoramento, houve a necessidade de analisar esse tráfego tão superior capturado pelas ferramentas. Para realizar essa análise no tráfego da placa de rede da estação Febe e descobrir o que realmente esta sendo acessado e baixado, foram utilizados os *sniffers Wireshark* e *Microsoft Network Monitor*. As duas ferramentas fizeram análises ao mesmo tempo para certificar os resultados da análise, observando que as duas ferramentas foram instaladas juntas com as três ferramentas de monitoramento, enquanto o MRTG, CACTI, e PRTG monitoraram e registravam o tráfego de entrada e saída de cada ativo, os *sniffers Wireshark* e *Microsoft Network Monitor* faziam a parte de análise desse tráfego, verificando e capturando os pacotes que estavam sendo enviados e recebidos pelos ativos em toda a rede.

Nos próximos 2 tópicos serão apresentados os dados coletados através das ferramentas de análise *Wireshark* e *Microsoft Network Monitor* sobre o tráfego

passante na placa de rede da estação Febe no momento em que houve maior tráfego de entrada na mesma.

3.9.5 **Dados Coletados pela Ferramenta Wireshark**

Conforme citado na apresentação do ambiente, a empresa possui um *hub switch* que tem por função interligar todas as estações de serviço da rede da organização. Uma das características do *hub switch* é que ele, antes de tudo, é um *hub.* Assim, ele envia todos os pacotes para todas as portas, e com isso todas as estações de serviço irão receber todos os pacotes. Para o *Wireshark* capturar os pacotes enviados e recebidos pelos ativos monitorados na empresa, ele poderia ser instalado em qualquer ativo da própria rede, pois todas irão receber os pacotes através do *hub switch* sem exceção. O *Wireshark* foi instalado no servidor Saturno e configurado para realizar a captura dos pacotes na própria interface de rede do servidor durante a semana de monitoramento. A ferramenta *Wireshark* apresentou uma grande gama de informações sobre o que estava sendo enviado e recebido de pacotes por cada estação na rede, e como o principal alvo da análise é a estação Febe, as informações referentes a esta foram isoladas e analisadas separadamente.

Conforme ilustrado na figura 9 o ativo Febe no intervalo em que houve o alto valor de tráfego de entrada, efetuou diversas solicitações e acessou inúmeros sites, entre estes um site de download chamado piratebay.org.

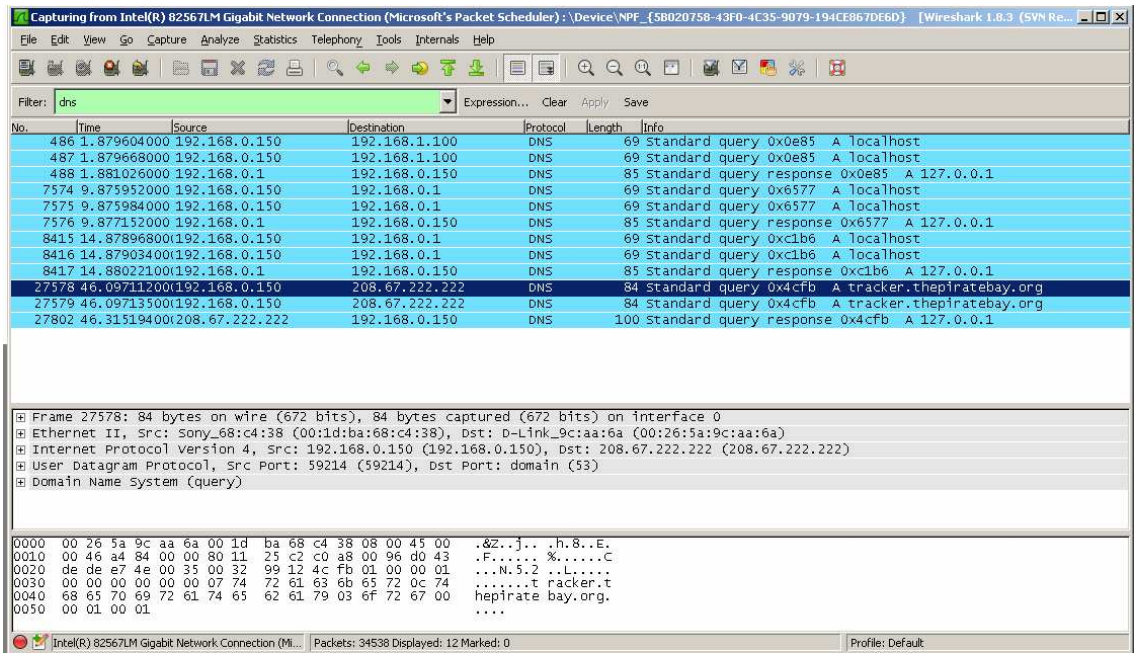


Figura 9 - Ilustra as solicitações dos ativos capturadas pelo Wireshark

3.9.6 **Dados Coletados pela Ferramenta Microsoft Network Monitor**

A ferramenta *Microsoft Network Monitor,* como a ferramenta *Wireshark*, foi instalada e configurada também no servidor Saturno, e iniciada para capturar os pacotes enviados e recebidos na rede durante toda a semana de monitoramento. Como no procedimento de análise das informações coletadas pelo *Wireshark*, também foram isoladas as informações sobre o ativo Febe e analisados os pacotes enviados e recebidos pela mesma estação. Conforme ilustrado na figura 10, é possível observar que o *Microsoft Network Monitor* detectou o acesso realizado através da estação Febe ao mesmo site de download apresentado pela ferramenta *Wireshark*.

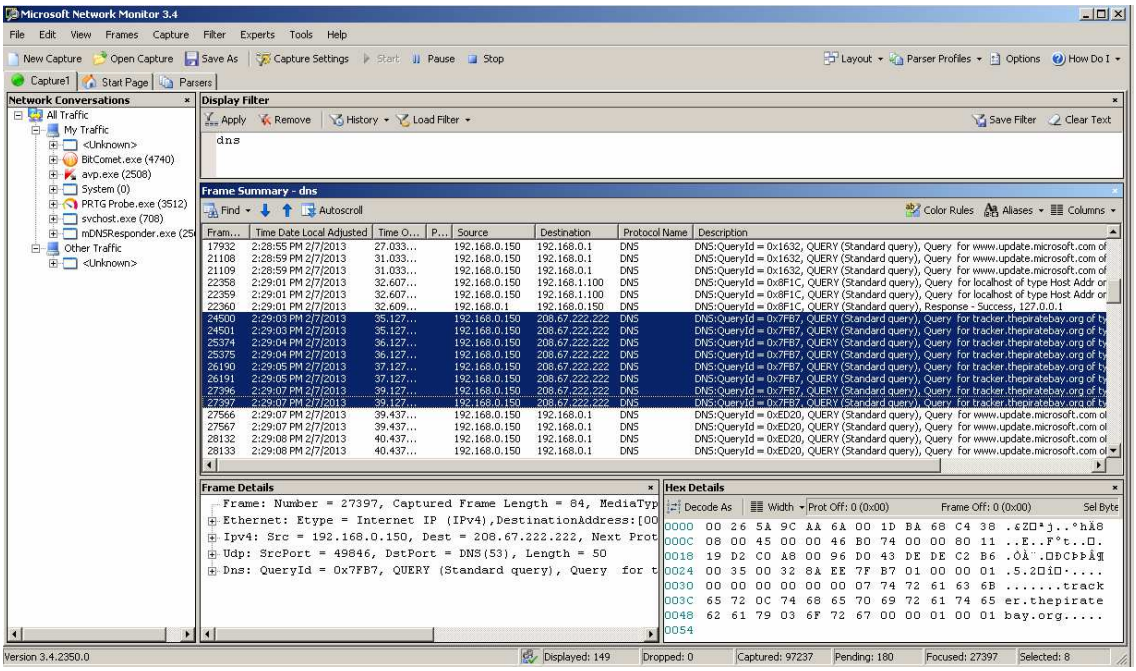


Figura 10 - Ilustra as solicitações dos ativos capturadas pelo Microsoft Network Monitor

3.9.7 **Análise do Resultado das ferramentas WIRESHARK e MICROSOFT NETWORK MONITOR**

As figuras 9 e 10 ilustram como as duas ferramentas de análise detectaram que o ativo Febe acessou inúmeros sites diferentes, tais como sites de jogos, filmes, entre outros, no mesmo intervalo em que houve o maior valor de tráfego de entrada apresentado pelas ferramentas de monitoramento. Houve acesso ao site de download apresentado nas duas figuras, e este trata-se de um programa de download de *torrents*. Após ser instalado é necessário fazer o download das *seeds*. No site de download percebeu-se que é lançado constantemente *seeds* e atualizações, e isso explica as várias solicitações de download para o site efetuadas pelo ativo Febe.

Com o auxilio das ferramentas de monitoramento e de análise foi identificado o ativo Febe como o causador da lentidão de acesso à *internet* ocorrido em vários

momentos durante a semana de monitoramento. Com isso, o próximo passo é solucionar essa lentidão resultante do uso inadequado pelos funcionários do setor de pesquisa. A política da empresa em questão é não bloquear sites ou restringir o acesso à internet pelos funcionários de todos os setores da organização, por isso o acesso à internet é totalmente liberado para todas as estações de serviço, sem exceção. Então por essa organização ter este tipo de política, e por consequência não podendo bloquear os downloads detectados pelas ferramentas de análise, a solução escolhida foi limitar o tráfego de entrada e saída de cada ativo da rede, de forma que nenhuma estação ultrapasse o limite de tráfego de entrada e saída definido.

3.9.8 **Uma Forma de Neutralizar o Problema**

Para limitar o tráfego de entrada e saída nas interfaces de rede das estações de serviço foram testadas várias soluções e diferentes métodos. O primeiro método consiste em aproveitar os próprios recursos disponíveis na organização para limitar o tráfego. A rede da empresa possui um *hub switch* 10/100 não gerenciável da marca *Encore.* Assim então foram verificadas as funcionalidades e o manual do *hub switch* disponível no site do fabricante para descobrir se esse tipo de equipamento oferece alguma função para limitar o tráfego de cada estação de serviço. Após análise e consulta do manual concluiu-se que o *hub switch* em questão não possui nenhuma funcionalidade, como por exemplo priorização de tráfego (QoS) simples, e também não possui a funcionalidade de priorização de trafego (QoS) avançado.

O segundo método testado foi utilizar uma ferramenta para efetuar esse controle de tráfego de uma forma centralizada, instalando esse *software* no próprio

servidor da empresa. Essas ferramentas que controlam a banda são chamadas limitadores ou modeladores de banda. Foram testados vários *softwares* para este fim, tais como *Bandwidth Controller* e *SoftPerfect Bandwidh Manager*, que são ferramentas pagas e recomendadas para o uso em redes onde as estações de serviço utilizam o sistema operacional *Microsoft Windows*. O *SoftPerfect Bandwidth* possui dois componentes, o primeiro é um serviço de sistema que deve ser instalado em uma máquina na rede que seja o *gateway* da internet, e o segundo é uma interface gráfica para o usuário final. O *Bandwidth Controller,* como o *SoftPerfect Bandwidth*, também precisa ser instalado numa máquina na rede que seja o *gateway* de *internet* para poder limitar o tráfego de entrada e saída de cada estação de serviço. Nenhum *software* cliente é necessário ser instalado nas estações de serviço na rede. O servidor Jupiter faz o papel de roteador e é o *gateway* de *internet* na rede e não o servidor Saturno. O grande problema desta instalação no *gateway* de internet é que o nosso *gateway* possui sistema operacional *Unix Freebsd* (conforme a figura 3). Com isso foi impossível utilizar as duas ferramentas citadas, pois para controlar o tráfego utilizando-as é necessário ter uma estação que seja o *gateway* de internet e possua sistema operacional compatível com ambiente *Windows* e essa condição não se aplica na rede da empresa.

O terceiro método testado para controlar o tráfego nas estações de rede foi a instalação de uma ferramenta limitadora de tráfego em cada estação de serviço. Para isso foi utilizada uma ferramenta livre chamada *NetBalancer*, que é um controlador de tráfego desenvolvido, conforme a documentação disponível no site da própria ferramenta, para controlar tráfego de estações de serviço que operam com o sistema operacional *Microsoft Windows*. Foi realizado o download do

NetBalancer no próprio site da ferramenta, onde está disponível uma versão gratuita. Para obtê-la basta acessar *http://www.seriousbit.com/netbalancer/* e efetuar o *download* do *NetBalancer Pro Free*. Antes da instalação da ferramenta nas estações de serviço foram analisadas suas funcionalidades disponíveis na versão gratuita, pois, conforme a documentação no site da própria ferramenta, a versão gratuita é limitada e permite controle apenas para cinco processos de prioridades e cinco regras para cada estação onde é instalada. Após a análise, verificou-se que a versão gratuita oferece uma opção que limita o tráfego de entrada e de saída de cada estação definindo uma cota de uso de banda para cada estação na rede, sem que seja necessário o uso de priorização ou a criação de regras. Com isso pode-se definir *download* e *upload* nas estações, impedindo o uso excessivo de banda, como o tráfego identificado nas tabelas 1, 2 e 3 na estação Febe. Para testar a funcionalidade citada acima, verificar e constatar que realmente é possível controlar e limitar o tráfego com o uso do *NetBalancer Pro Free*, o próximo passo foi instalá-lo em cada estação, e definir o valor máximo de *download* e *upload* que cada estação poderia atingir.

3.9.9 **Ação para Neutralizar o Problema Encontrado**

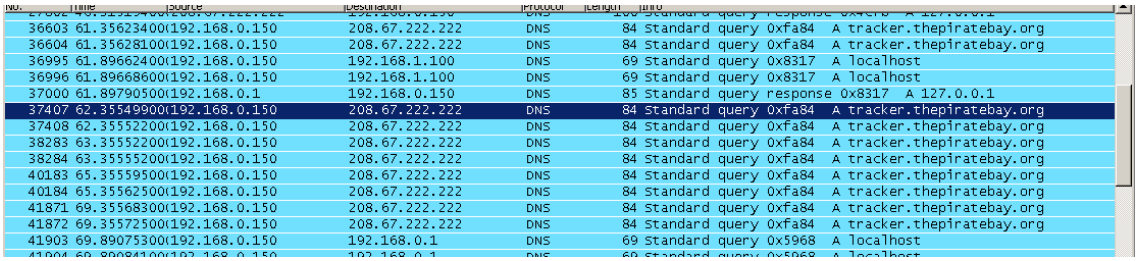
A organização possui um enlace não dedicado de 100 Mbps T1 LAN oferecido pela universidade, e por ser um *link* não dedicado significa que as velocidades de *download* e *upload* não são fixas e mudam constantemente. A fim de distribuir a velocidade de *download* e *upload* de forma igual entre as doze estações da rede foram definidas no *NetBalancer* os valores 64 KBps de *download* e 42,7 KBps de *upload*. Com o *NetBalancer* configurado corretamente com os valores a cima, o tráfego de entrada e de saída na placa de rede da estação Febe

foi monitorado para verificar se realmente a ferramenta limitadora de banda cumpriu com o seu objetivo. Após analisar os valores apresentados pelas ferramentas de monitoramento foi constatado que realmente houve o controle de tráfego esperado.

No próximo capítulo serão apresentados os gráficos gerados pelas ferramentas MRTG, CACTI, e PRTG, comprovando o sucesso em controlar o *download*, e com isso eliminar o uso excessivo de banda pela estação Febe ou por qualquer outra estação.

4 RESULTADOS

A figura 11 ilustra uma solicitação de *torrents* efetuada pela estação Febe após a instalação do controlador de tráfego *NetBalancer*. Essa solicitação foi realizada entre as 14h e 16h, e deu início ao *download* que será monitorado pelas ferramentas de monitoramento no mesmo período nas figuras 13, 15 e 17.



36603	61.35623400	192.168.0.150	208.67.222.222	DNS	84 Standard query 0xfa84 A tracker.thepiratebay.org
36604	61.35628100	192.168.0.150	208.67.222.222	DNS	84 Standard query 0xfa84 A tracker.thepiratebay.org
36995	61.89662400	192.168.0.150	192.168.1.100	DNS	69 Standard query 0x8317 A localhost
36996	61.89668600	192.168.0.150	192.168.1.100	DNS	69 Standard query 0x8317 A localhost
37000	61.89790500	192.168.0.1	192.168.0.150	DNS	85 Standard query response 0x8317 A 127.0.0.1
37407	62.35549900	192.168.0.150	208.67.222.222	DNS	84 Standard query 0xfa84 A tracker.thepiratebay.org
37408	62.35552200	192.168.0.150	208.67.222.222	DNS	84 Standard query 0xfa84 A tracker.thepiratebay.org
38283	63.35552200	192.168.0.150	208.67.222.222	DNS	84 Standard query 0xfa84 A tracker.thepiratebay.org
38284	63.35555200	192.168.0.150	208.67.222.222	DNS	84 Standard query 0xfa84 A tracker.thepiratebay.org
40183	65.35559500	192.168.0.150	208.67.222.222	DNS	84 Standard query 0xfa84 A tracker.thepiratebay.org
40184	65.35562500	192.168.0.150	208.67.222.222	DNS	84 Standard query 0xfa84 A tracker.thepiratebay.org
41871	69.35568300	192.168.0.150	208.67.222.222	DNS	84 Standard query 0xfa84 A tracker.thepiratebay.org
41872	69.35572500	192.168.0.150	208.67.222.222	DNS	84 Standard query 0xfa84 A tracker.thepiratebay.org
41903	69.89075300	192.168.0.150	192.168.0.1	DNS	69 Standard query 0x5968 A localhost

Figura 11 - Solicitação de download realizada pela estação Febe

A figura 12 mostra o gráfico gerado pela ferramenta MRTG sobre o tráfego de entrada e de saída na estação Febe antes da instalação e o uso da ferramenta *NetBalancer*. Como demonstrado na própria figura, o tráfego de entrada alcançou 519,4 KB/s.

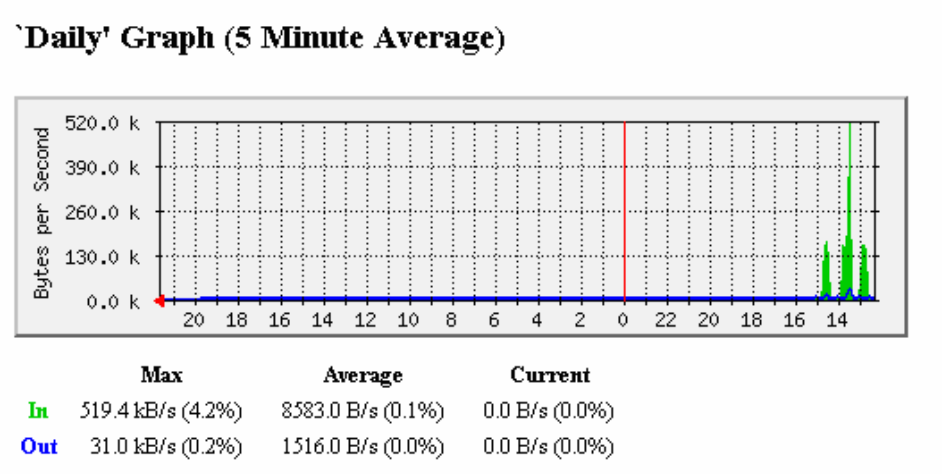


Figura 12 - Gráfico gerado pela MRTG antes do uso da *NetBalancer*

A figura 13 mostra o gráfico gerado pela ferramenta MRTG após a

implementação da ferramenta *NetBalancer*. Percebeu-se que o tráfego de entrada alcançou 63,4 KB/s, e não ultrapassou o valor máximo de *download* definido em 64 KB/s.

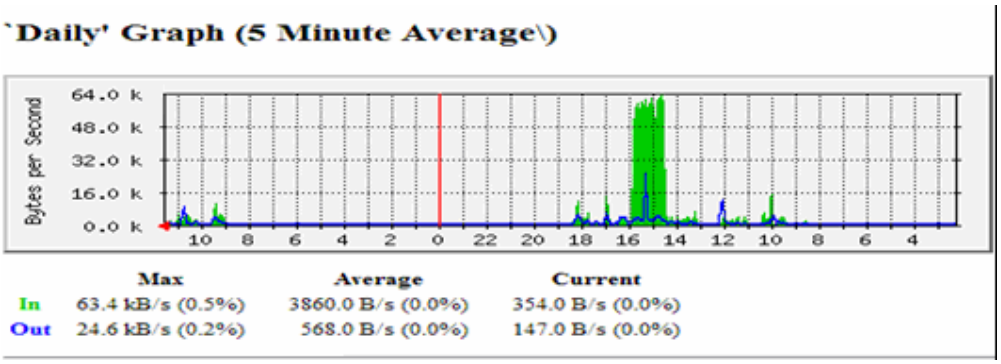


Figura 13 - Gráfico gerado pela MRTG comprovando o controle de tráfego

O gráfico ilustrado na figura 14 foi gerado pela ferramenta CACTI antes da implementação da ferramenta *NetBalancer*, no mesmo intervalo de monitoramento da figura 12.

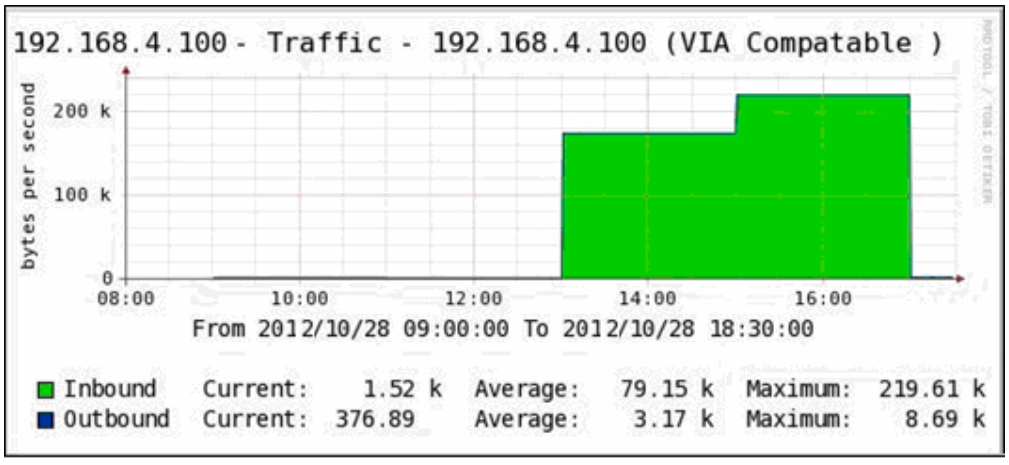


Figura 14 - Gráfico gerado pela CACTI antes do uso da NetBalancer

A figura 15 apresenta um gráfico que foi gerado pela ferramenta CACTI

após a instalação da ferramenta NetBalancer. O valor máximo de tráfego de entrada alcançou 61,79 KB/s e não ultrapassou o valor definido em 64 KB/s.

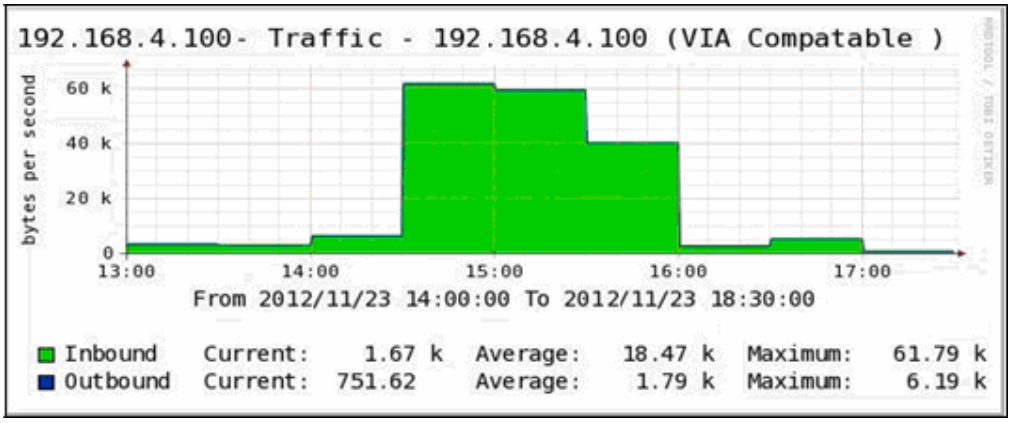


Figura 15 - Gráfico gerado pela CACTI comprovando o controle de tráfego

A figura 16 demonstra um gráfico que foi gerado pela ferramenta PRTG antes da implementação da ferramenta NetBalancer. O valor máximo 6.650,00 Kbit/s ilustrado neste gráfico, e que equivale 831,25 KB/s, representa o tráfego total de entrada e de saída registrado pela ferramenta PRTG no mesmo intervalo de monitoramento ilustrado nas figuras 12 e 14.

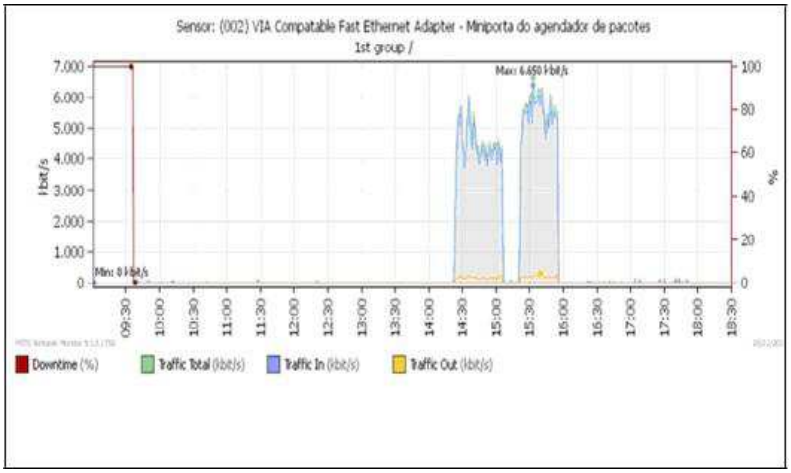


Figura 16 - Gráfico gerado pela PRTG antes do uso da *NetBalancer*

O gráfico gerado pela ferramenta PRTG após a implementação da ferramenta *NetBalancer* é ilustrado na figura 17. Ele mostra que houve controle de tráfego de entrada, pois o valor máximo alcançado foi 500 Kbit/s que equivale 62,5 KB/s.

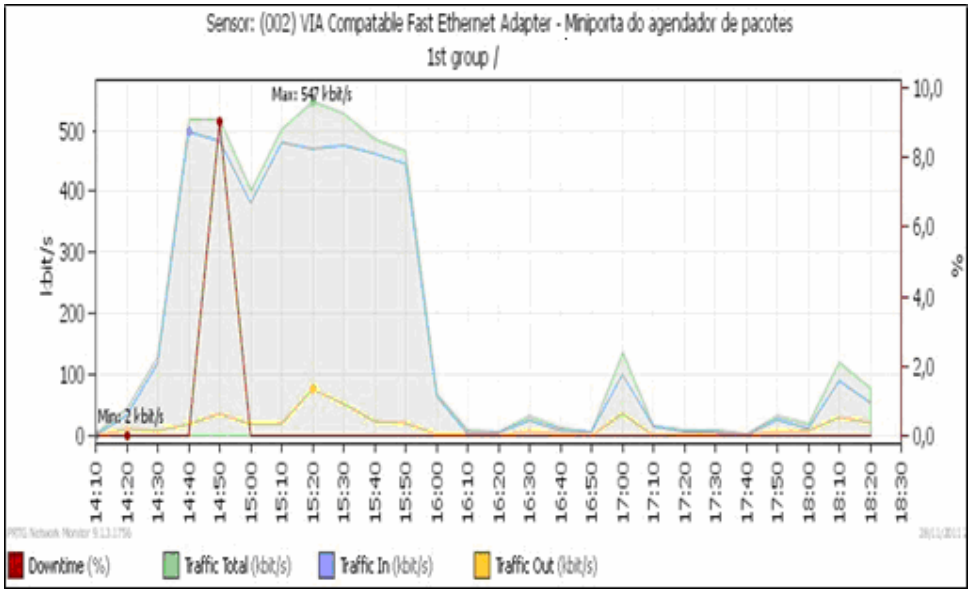


Figura 17 - Gráfico gerado pela PRTG comprovando o controle de tráfego

Portanto, como ilustrado nas figuras 13 e 15, este gráfico também comprova que não foi ultrapassado o valor definido em 64 KB/s para download.

5 CONCLUSÃO

Conforme ilustrado nesta monografia, foi comprovada a importância da utilização de várias ferramentas de gerência de redes trabalhando em conjunto para chegar a um objetivo desejado, que neste caso é identificar a falha que prejudicava o desempenho da rede da empresa, causando lentidão de acesso à *internet*. Enquanto as ferramentas de análise gráfica de comportamento da rede e os dispositivos monitoravam o tráfego e identificavam o ativo causador do consumo excessivo da banda, as ferramentas de análise de pacotes interceptavam e registravam o tráfego de dados na rede e mostravam o que estava sendo acessado e qual o ativo problemático, identificando os *downloads* realizados pela estação Febe.

Com o uso do modelador de tráfego *NetBalancer*, foi possível limitar a banda para qualquer tráfego, não apenas aos sites de *downloads*, e com isso neutralizar o problema e solucionar a lentidão e as quedas constantes de conexão de internet que prejudicavam o desempenho e a produção da empresa. Por ser uma ferramenta livre, a empresa se beneficiou de uma solução gratuita sem ser necessário investir na compra de um *software*. Porém, este método de controlar o tráfego instalando o *NetBalancer* em cada estação de serviço é vulnerável, pois nada impede que os usuários com maior conhecimento desinstalem a ferramenta ou efetuem alterações. Sendo assim, para solucionar esta situação foi desativado o painel de controle das estações de serviço, e com isso os usuários ficaram impossibilitados de desinstalar programas sem autorização. Foi também utilizado o método de distribuição do *software* de limitação de tráfego via *Group Policy*, utilizando o *Active Directory* no servidor Saturno.

Uma das dificuldades encontradas durante o desenvolvimento do trabalho

foi a carência de recursos financeiros para investimentos em equipamentos que oferecem mais funcionalidades, tais como *switches* que possuem QoS avançado e que sejam gerenciáveis.

No próximo ano a empresa avaliada possui planos para expansão, aumentando o número das estações de serviço e o quadro de funcionários em todos os setores, o que tornaria trabalhoso e demorado o método utilizado nesta monografia para controlar o tráfego em cada estação de serviço através da instalação do modelador *NetBalancer*. Assim, foi informado ao setor responsável a importância e a necessidade de aquisição de um *switch* gerenciável substituindo o atual *hub switch*, pois com sua aquisição o controle de tráfego se tornaria mais fácil, rápido e seguro. O uso de um *switch* gerenciável oferece várias vantagens se comparado ao não gerenciável, entre estas, a possibilidade de priorização de tráfego, que é o ideal para aplicações como VoIP (Voice Over Internet Protocol) e multimídia, como também controlar a banda por porta, evitando que uma estação na rede consuma toda a banda como ocorria no exemplo dado nesta monografia pela estação Febe.

REFERÊNCIAS

[1] BLACK, Lovis Tomas. Comparação de ferramentas de gerenciamento de Rede. Rio de Janeiro: UFRGS Dezembro 2008.

[2] CACTI. Disponível em: <http://www.cacti.net> . Acesso em: 05 Out. 2012

[3] CARVALHO, Tereza Cristina Melo de Brito. Gerenciamento de Redes: Uma abordagem de sistemas abertos. – Elaboração. São Paulo: ABNT, 1993.

[4] HARNEDY, Sean. Total SNMP: Exploring the Simple Network Management Protocol. 2 ed. Prentice Hall PTR, 1997.

[5] INTERNET ENGINEERING TASK FORCE. Disponível em: <http://www.ietf.org>. Acesso em: 01 Set. 2012.

[6] KUROSE, J. ROSS, W. K. Redes de Computadores e a Internet – Uma Abordagem Top Down 3ª Edição. Pearson. 2005.

[7] MAURO, Douglas R. SCHMIDT, Kevin J. SNMP Essencial. Rio de Janeiro: Campus 2001. MICROSOFT NETWORK MONITOR. Disponível em: <http://social.technet.microsoft.com/wiki/contents/articles/4529.aspx>. Acesso em: 22 Out. 2012

[8] MRTG. Disponível em: < http://oss.oetiker.ch/mrtg/>. Acesso em: 02 Out. 2012

[9] PRTG. Disponível em: <http://www.paessler.com/prtg>. Acesso em: 20 Out. 2012

[10] STALLINGS, William. SNMP, SNMPv2 and RMON: Practical Network Management Second Edition. Massachusetts: 1996.

[11] TANENBAUM, Andrew S. Redes de computadores. 4ª Ed., Rio de Janeiro: Editora Campus, 2003.

[12] WIRESHARK. Disponível em: <http://www.wireshark.org/docs/>. Acesso em: 18 Out. 2012